# Section 10

# INTERFACES

## Contents

Introduction ........ 10-1
Integration by the Physical Security Systems Topic Team ........ 10-2
Classified Matter Protection and Control ........ 10-2
Personnel Security ........ 10-4
MC&A ........ 10-4
Protective Force ........ 10-4
Computer Security ........ 10-5

## Introduction

Integration is the coordination and cooperation among inspection team members designed to achieve a more effective and organized inspection effort. It creates a synergism that results in an enhanced knowledge of the inspected site, a strengthening of inspection techniques, and a more comprehensive inspection report. The integration effort significantly contributes to the effectiveness of the OA-10 inspection process and, along with other unique attributes, enhances OA-10's ability to provide an accurate, in-depth evaluation of protection programs throughout the DOE complex.

Because of the interdependency of elements of any security system, integration must continue throughout all phases of the inspection to ensure that all pertinent data has been shared. Integration, facilitated by one or more integration teams, is realized by exchanging information and discussing how information collected by one topic team influences the performance of security system elements observed by other topic teams. The fundamental goal of this effort is to ensure that potential systemic vulnerabilities are clearly identified and analyzed.

In addition to enhancing inspection results, integration has several other major benefits. First, it allows topic teams to align their efforts so that their activities complement rather than detract from one another. It is usually less productive to inspect PSSs at one location, control classified documents and material at a different location, and the protective force at yet another location. Using this approach, inspectors would accumulate a collection of unrelated facts. Therefore, topic teams must cooperate to make the best choices regarding what should be inspected at which locations. Early and continuing integration helps ensure that the activities of all topic teams are unified and contribute to the overall goal.

A second benefit of integration is that it allows topic teams to benefit from the knowledge, experience, and efforts of other topic teams. Sometimes, ideas developed by one topic team can help another topic team focus inspection activities in a more productive and meaningful direction. For example, the PSS topic team may indicate that its planning effort led to the conclusion that the physical systems at a particular location are weak, resulting in heavy reliance on the protective force. It may therefore be useful for the protective force topic team to plan to spend more time assessing protective force capabilities as they relate to this weakness, rather than spending a lot of time examining other areas.

The third benefit of integration is to prevent topic teams from interfering with each other. Often, several topic teams concentrate their activities at the same location, resulting in multiple visits over time or a number of visits at the same time. This causes undue disruption of the facility being inspected. Integration among topic teams can preclude this problem by having one or two topic teams visit a particular location and collect the data for several. All topic teams should be aware of what all other topic teams are doing, where they are doing it, and how it will affect their own activities.

Integration of data-collection activities for performance testing is imperative. If the PSS topic team schedules a performance test that results in the activation of the alarm system in a building, and MC&A topic team schedules a performance test involving an emergency inventory or transfer of material in the same building at the same time, the resulting problem is obvious.

## Integration by the Physical Security Systems Topic Team

PSSs are an integral part of the overall protection program at any DOE facility, and therefore must interact with other elements of that program. Therefore, the topic cannot be inspected in isolation. Inspection team members must continually keep this in mind in order to determine how well this interaction works. This requires integration with inspection teams responsible for other areas. Information developed by these teams may affect how the results of the PSS team efforts are viewed. Similary, data gathered by the PSS team may have some bearing on how the results of another team's efforts are viewed.

Figure 3 shows the common areas of interface for the PSS topic with other topics.

### Classified Matter Protection and Control

The classified matter protection and control (CMPC) topic relates to PSS because of requirements for protecting classified information and material. Some protective measures common to PSS and CMPC are:

- Control and storage of documents
- Physical control of classified parts
- Establishment of security areas for classified information processing, including secure communications centers
- Alarm log printouts, alarm system drawings, and compensatory plans.

Aspects of the physical protection program that are normally reviewed by the PSS or protective force teams and are normally **not** included within the scope of the CMPC review include:

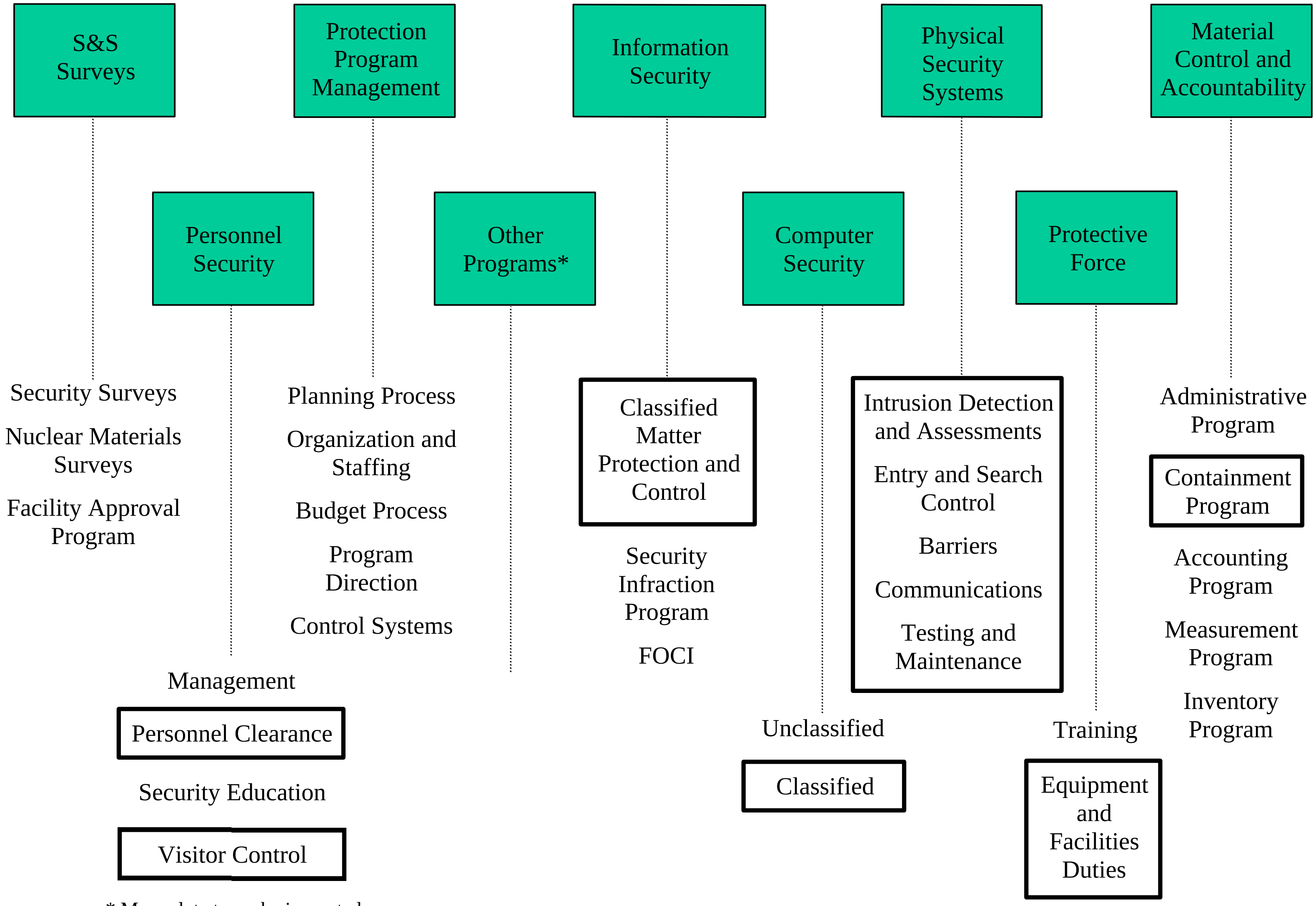
- Technical aspects of alarm systems (e.g., tamper capabilities)
- CAS operations
- Search equipment sensitivity
- Security hardware testing or maintenance.

Aspects of the physical protection program that the CMPC team would typically include within the scope of its review include:

- Physical protection during transfers
- Storage of keys and combinations
- Lock combination change procedures
- Repository checks.

The following aspects of the physical protection program are normally reviewed by the PSS team, but could be reviewed by the CMPC team instead if circumstances warrant (e.g., if the other teams have different priorities and do not plan detailed reviews of the elements of interest to the CMPC team):

- Alarm sensor operability and coverage
- Use of appropriate locks
- Access controls and barriers at limited or exclusion areas
- Search procedures at limited or exclusion areas



* May relate to, or be inspected under, one or more topic areas.

**Figure 3. Areas of Interface Most Common to the Physical Security Systems Topic Team**

- Protective force patrols (may also be reviewed by the protective force team)

- Badge and pass systems.

### Personnel Security

Elements of personnel security must be considered by the PSS topic team when the site places high reliance on the adequacy of the personnel security programs. Implementation of human reliability or personnel security assurance programs may directly affect the overall PSS program. Also, PSS may interface with personnel security in the areas of visitor control and escort procedures.

### MC&A

The interface between the inspection of PSS and MC&A is important to ensure that findings are reported in the appropriate topic are and that both inspection teams are aware of potential problem areas impacting their individual conclusions. DOE orders require that MC&A procedures be compatible with the physical protection and security of the system.

The PSS and MC&A topics overlap in a number of areas, including:

- Surveillance of SNM

- Access controls and records

- MAAs

- Portal monitors

- Material transfers

- Storage of materials

- Detection of unauthorized activity or conditions

If both topics are inspected at the same facility, any findings involving areas of overlap should be coordinated between the MC&A and PSS topic teams to ensure that findings are reported under the most appropriate topic.

Typical findings of mutual interest include:

- Deficiencies in barriers that could allow an insider to divert material outside of a security area without detection

- Access controls that do not meet DOE requirements

- Deficiencies in the intrusion-detection system protecting SNM storage repositories or security area perimeters

- Deficiencies in locks, key control, or combination controls, which indicate an insider could gain unauthorized access to SNM

- Portal monitor capabilities that are ineffective or not consistent with the type of material in the MAA

- Inadequate implementation of procedures, such as the two-person rule or vault closing/operating procedures

- Category I quantities of SNM stored outside a vault or vault-type room.

The interface with the MC&A topic team can frequently result in identifying locations of special concern due to the category or attractiveness of material in process or storage. This information can significantly redirect the focus of the PSS inspection. For example, if a significant quantity of SNM is identified as being outside the MAA during inspection planning, it may initially be considered a major problem. However, subsequent coordination between the MC&A team and the systems team may reveal that there is no problem due to the condition of the material and the storage method. In this case, both teams can refocus their attention and inspection activities.

### Protective Force

Interface with the protective force topic team is very important in performance testing.

In addition, the subtopic of badges, passes, and credentials is of interest to a variety of OA-10 inspection teams (typically, personnel security, CMPC, and protective force). Usually, the PSS team reviews the badge system; however, the personnel security, protective force, and CMPC topic teams must be kept informed of results, because they may also review some aspects of the badge system. For example, the personnel security team may review the procedures for issuing badges, and the protective force topic team often observes badge-checking procedures at portals. Performance tests conducted by protective force inspectors also have a bearing on any conclusion drawn by PSS inspectors. Consequently, all of these topic teams must coordinate their efforts both to assure full coverage and to avoid duplication of effort.

The PSS team can increase the efficiency of their data collection efforts by having the protective force team help collect data at the portals. For example, the PSS inspectors could provide the protective force inspectors with a short list of information to gather at each post as part of the post checks. Examples of information that might be more efficiently collected by the protective force team include whether the SPOs are knowledgeable about policies for accepting badges of other contractors, whether each post has a current list of lost badges, and whether the post orders are consistent with site policies.

### Computer Security

The interface with computer security routinely involves an evaluation of the effectiveness of security controls implemented on computer systems used to operate automated access controls systems, intrusion-detection systems, and video-monitoring systems. This interface is especially important because many facilities do not consider the data processed by these computers to be classified. Therefore, the computers are not subject to the same strict security requirements as classified systems. This could lead to falsification of access credentials, unauthorized database manipulation, or, in the worst case, undetected defeat of intrusion detection for an MAA. Because of the diversity of security alarm system applications, it is important that the PSS team works closely with the computer security team to determine the required level of protection that the security alarm system is expected to provide, and to evaluate the computer’s ability to meet that end.

This page is intentionally left blank.